nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

## Enable trusted paperless processes and secured digital cross-border business throughout Europe

- Support digital signing, authentication, and encryption
- Provide secure electronic signature with full legal validity
- Facilitate free circulation of digital documents across EU
- Maximize flexibility through web and mobile capabilities
- Build root of trust with a secure signature creation device

INTESI GROUP

# INTESI GROUP and nCipher provide eIDAS compliant remote signature solution

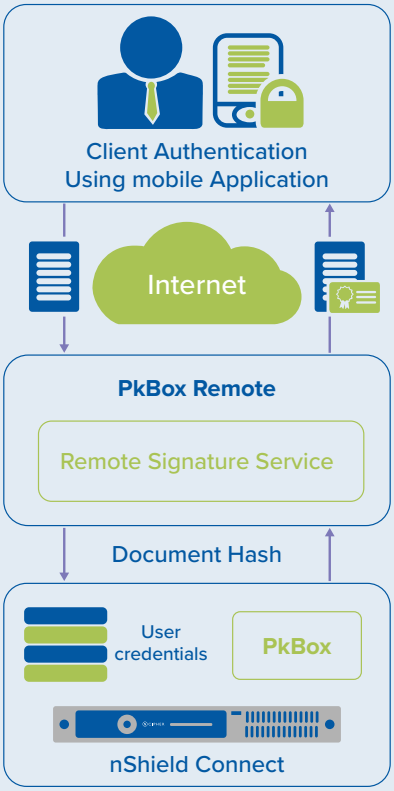
### THE PROBLEM: CONTINUED USE OF VULNERABLE ONLINE SERVICES TO CONDUCT LEGALLY-BINDING TRANSACTIONS

Today, more and more business is conducted online through digital paperless means. When a legally-binding transaction is executed remotely, trusted mechanisms recognized by all parties involved must be in place to ensure legitimacy and non-repudiation.

Digital signatures have filled this need, but a common standard is necessary for the legal certainty of trust services across a common market.

### THE CHALLENGE: DELIVERING A FLEXIBLE, SCALABLE, AND TRUSTED SERVICE FOR DIGITAL CROSS-BORDER BUSINESS

The regulation on electronic identification and trust services for electronic transactions (eIDAS) establishes the common standard that enables legally-binding cross-border business across Europe. eIDAS compliant Qualified Signature Creation Devices (QSCDs) enable users to remotely sign transactions and documents. To ensure that the electronic signatures receive the same legal recognition as those created in traditional user-managed environments, trustworthy systems and channels must be used to guarantee reliability and control, including use of cryptography and the protection of associated signing keys.




nCipher nShield integrates with INTESI GROUP PkBox to safeguard and manage the cryptographic keys used to support the signing process.

# INTESI GROUP and nCipher provide eIDAS compliant remote signature solution

## THE SOLUTION: LEGALLY RECOGNIZED REMOTE ELECTRONIC SIGNATURES WITH A STRONG CRYPTOGRAPHIC ROOT OF TRUST

INTESI GROUP PkBox security server is a QSCD designed for high volume transactional environments. When used with qualified certificates, PkBox generates legally-binding Qualified Electronic Signatures and Qualified Electronic Seals. The solution enables public and private organizations from industries such as banking, insurance, and healthcare to capitalize on the opportunities brought by eIDAS Regulation EU 910/2014 regarding the implementation of paperless processes and digital cross-border business. PkBox can be used for signature and seal creation, verification, authentication, and encryption. The solution offers high performance, resiliency, and scalability. Capable of managing millions of signature credentials and one-time passwords (OTPs), the solution can easily scale in a load-balanced multi-tiered architecture. PkBox supports in-house deployments, as well as remote signatures base on INTESI GROUP Time4Mind cloud service.

INTESI GROUP PkBox integrates with nCipher nShield hardware security modules (HSMs) to safeguard and manage the cryptographic keys used to support the signing process. The result is a certified high performance solution able to handle large volumes of transactions with maximum flexibility.

## WHY USE NCIPHER NSHIELD HSMs WITH INTESI GROUP PKBOX?

Signing keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical data. HSMs are the only proven and auditable way to secure cryptographic material. nShield HSMs integrate with PkBox to safeguard security sensitive information including OTP seeds, signature keys, and authentication passwords. The HSM provides comprehensive logical and physical protection, delivers an auditable method for enforcing security policies, and builds a strong root of trust with a secure signature creation device.

nCipher nShield Connect HSMs enables INTESI GROUP PkBox customers to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the QSCD
- Deliver superior performance to support demanding transaction volumes

## NCIPHER - AN ENTRUST DATACARD COMPANY

nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nCipher HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

## INTESI GROUP

PkBox provides state of the art remote electronic signature, data encryption, and strong authentication. Thanks to its scalable and flexible architecture, PkBox enables a software factory to:

- Manage any kind of security tasks (key management, electronic signature, verification, and time stamping) without the need of knowing the underlining technologies
- Develop solution to manage millions of credentials and certificates with the required throughput of signatures , seals, and authentications
- Comply with eIDAS regulation and manage security operations with the keys protected in a nCipher HSM

For more detailed technical specifications, please visit www.ncipher.com or www.intesigroup.com